UNC SCHOOL OF LAW

NORTH CAROLINA LAW REVIEW

Volume 92
Number 5 *Health Care Decisions in the New Era of Health Care Reform*

Article 8

6-1-2014

Private Certifiers and Deputies in American Health Care

Frank A. Pasquale

PRIVATE CERTIFIERS AND DEPUTIES IN AMERICAN HEALTH CARE*

FRANK A. PASQUALE**

So-called "public programs" in U.S. health care pervasively contract with private entities. The contracting does not merely involve the purchase of drugs, devices, information technology, insurance, and medical care. Rather, government agencies are increasingly outsourcing decisions about the nature and standards for such goods and services to private entities. This Article will examine two models of outsourcing such decisions. In private licensure, firms offer a stamp of approval to certify that a given technology or service is up to statutory or regulatory standards. Via deputization, firms can pursue a regulatory or law enforcement role to correct (and even punish) providers who have failed to meet standards or acted fraudulently. Both private licensure and deputization provide new models for administrative governance in rapidly changing, technically complex fields. But they can also be abused if private licensors or deputies are not adequately supervised, or if they are faced with too crude an incentive framework. This Article suggests some best practices for the outsourcing of responsibility to these health care decision makers.

** Professor of Law, University of Maryland School of Law. I wish to thank Richard Saver and Joan Krause for inviting me to the *North Carolina Law Review*'s excellent symposium on decision making in American health law. Elizabeth Clark Rinehart and Melanie Dang provided expert and diligent research support for this project.

INTRODUCTION

So-called "public programs" in U.S. health care pervasively contract with private entities. The contracting does not merely involve the purchase of drugs, devices, information technology, insurance, and medical care. Rather, government agencies are increasingly outsourcing decisions about the *nature and standards for such goods and services* to private entities. This Article will examine two models of outsourcing such decisions. In *private certification*, firms offer a stamp of approval to certify that a given technology or service is up to statutory or regulatory standards. Via *deputization*, firms can pursue a regulatory or law enforcement role to correct (and even punish) providers who have failed to meet standards or acted fraudulently. Both private certification and deputization provide new models for administrative governance in rapidly changing, technically complex fields. But they can also be abused if private licensors or deputies are not adequately supervised or if they are faced with too crude an incentive framework. This Article reviews critiques of the outsourcing of responsibility to these health care decision makers and concludes with a suggestion of converging technological developments and legal demands.

The degree of Centers for Medicare and Medicaid Services ("CMS") oversight of contractors burst into the headlines in October of 2013, when failures of the HealthCare.gov website highlighted conflictual relationships among CMS and the contractors responsible for developing and implementing the federal health insurance exchange.[1] While much of the critical media coverage of the Patient Protection and Affordable Care Act ("ACA") rollout has been

1. David Auerbach, *The Uninsured Are Now Unpaid Alpha Testers for the Government*, SLATE (Oct. 30, 2013, 10:36 AM), http://www.slate.com/articles/technology/bitwise/2013/10/healthcare_gov_tech_surge_the_uninsured_are_now_unpaid_alpha_testers_for.html.

unfair,[2] even the most steadfast defenders of the Obama administration were deeply disappointed by the rollout of HealthCare.gov. Former programmer David Auerbach has diagnosed some serious issues in government-contractor interrelationships that fed into the fiasco and the ongoing problems with fixing it.[3] For Auerbach, one of the critical faults here was that, "not only was very little testing done, but testing *frameworks* . . . weren't set up."[4] This was a fault not only of contractors, but of basic oversight over their implementation of critical information technology infrastructure.[5]

Ironically, the U.S. government already has fostered the development of a rigorous set of standards for the testing of information technology vendors' software—before the providers that buy it can obtain "meaningful use" subsidies for health information technology ("HIT").[6] Admittedly, on one level, this is an apples and oranges comparison: software for providing actual care is different than software that guides people through a maze of agencies, insurers, and data brokers.[7] On the other hand, the testing and certification of

2. *See* Tommy Christopher, *CNN's Jake Tapper and Elizabeth Cohen Try to Be Fair About Obamacare 'Sticker Shock,'* MEDIAITE (Oct. 30, 2013, 12:30 PM), http://www.mediaite.com/tv/cnns-jake-tapper-and-elizabeth-cohen-try-to-be-fair-about-obamacare-sticker-shock/.

3. Auerbach, *supra* note 1 ("[As of October 30, 2013,] only 30 percent [of users] have been able to complete an actual insurance application. And that's not even to say that the application is correct, owing to reports of children getting listed as multiple spouses and the like.... [W]hy on earth is the website still up? So people can play insurance-application roulette with 7–3 odds against them? Why not take the site down until it works?").

4. *Id.* ("That means the team fixing healthcare.gov not only has a lot of bugs to fix, but they don't have infrastructure in place to *identify* and . . . *reproduce* the bugs, which are the first step to fixing them. Under a tight deadline, any such infrastructure will be ad hoc and inadequate.").

5. *See* Alex Howard, *What Went Wrong at Healthcare.gov?*, DIGIPHILE (Dec. 1, 2013), http://digiphile.wordpress.com/2013/10/17/what-went-wrong-at-healthcare-gov/ ("[A] combination of procurement problems, poor work by a key contractor, bad management skills, insularity and political sensitivity led to a bug-laden website with a broken backend.").

6. *See generally What is ONC-Authorized Testing and Certification Body (ONC-ATCB)?*, HEALTH IT, http://www.healthit.gov/providers-professionals/faqs/what-onc-authorized-testing-and-certification-body-onc-atcb (last visited May 7, 2014) (describing Authorized Testing and Certification Bodies as set out by the Office of the National Coordinator for Health Information Technology, which "test and certify that certain types of electronic health record (EHR) technology (Complete EHRs and EHR Modules) are compliant with the standards, implementation specifications, and certification criteria adopted by the U.S. Department of Health and Human Services (HHS) Secretary and meet the definition of 'certified EHR technology' ").

7. *Compare* Becca Morn, *A Disheartening Visit to Healthcare.gov*, AMERICABLOG (Oct. 23, 2013, 7:00AM), http://americablog.com/2013/10/disheartening-visit-healthcare-gov.html (discussing user experience with the HealthCare.gov website), *with* Philip

HIT involves a multistep process of delegation that may well have been appropriate in the context of the federal exchange's development. The larger, common issue is that a federal government that has become so reliant on contractors may be losing its ability to assess the functionality and value of contractors' handiwork.[8]

The stakes of increased digitization and automation in health care are high.[9] A false record can be used *deliberately* to "bill . . . for a service not rendered" or provide the basis for "upcoding."[10] Moreover, it can be multiplied easily, given functionalities like one-click notes, copy and paste features, and billing-decision message prompts.[11] Both to encourage accurate records and to diminish

---

Longman, *Code Red: How Software Companies Could Screw Up Obama's Health Care Reform*, WASH. MONTHLY (July/Aug. 2009), http://www.washingtonmonthly.com/features/2009/0907.longman.html (discussing challenges to implementing electronic health care management software), *and* Steve Lohr, *Seeing Promise and Peril in Digital Records*, N.Y. TIMES, July 17, 2011, at BU3 (same), *and Bad Health Informatics Can Kill*, EFMI WG ASSESSMENT OF HEALTH INFO. SYS. (Oct. 19, 2012), http://iig.umit.at/efmi/badinformatics.htm (documenting issues with HIT systems that had real-world effects).

8. *See* JODY FREEMAN & MARTHA MINOW, GOVERNMENT BY CONTRACT: OUTSOURCING AND AMERICAN DEMOCRACY 1–3 (2009); *see also* Richard J. Pierce Jr., *Outsourcing Is Not Our Only Problem*, 76 GEO. WASH. L. REV. 1216, 1216–18 (2008) (reviewing PAUL R. VERKUIL, OUTSOURCING SOVEREIGNTY: WHY PRIVATIZATION OF GOVERNMENT FUNCTIONS THREATENS DEMOCRACY AND WHAT WE CAN DO ABOUT IT (2007)).

9. *See* Reed Abelson et al., *Medicare Bills Rise as Records Turn Electronic*, N.Y. TIMES, Sept. 22, 2012, at A1. Moreover, "[w]ithout a deliberate effort to build fraud management into [electronic systems], healthcare payers and consumers will be exposed to new and potentially increased vulnerability to electronically-enabled healthcare fraud." FOUND. OF RESEARCH AND EDUC. OF AM. HEALTH INFO. MGMT. ASS'N ("AHIMA"), REPORT ON THE USE OF HEALTH INFORMATION TECHNOLOGY TO ENHANCE AND EXPAND HEALTH CARE ANTI-FRAUD ACTIVITIES 13 (2005), *available at* http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_031699.pdf.

10. "Billing for services not rendered" is a scheme wherein a bill is deliberately submitted for payment even though no medical service was actually provided. FED. BUREAU OF INVESTIGATION, FINANCIAL CRIMES REPORT TO THE PUBLIC: 2010-2011, *available at* http://www.fbi.gov/stats-services/publications/financial-crimes-report-2010-2011. "Upcoding," by contrast, is a scheme wherein the health care provider submits a bill using a procedure code that yields a higher payment than the code for the service that was truly rendered. *Id.* It is important to distinguish these two schemes, which are committed deliberately, with inadvertent errors in coding for which, according to the *Wall Street Journal*, "[t]here are no comprehensive statistics . . . ." *See* Jessica Silver-Greenberg, *How to Fight a Bogus Bill*, WALL ST. J., Feb. 19, 2011, at B7, *available at* http://online.wsj.com/news/articles/SB10001424052748703312904576146371931841968 (discussing those who deliberately abuse Electronic Health Record software tools to commit health care fraud faster and with greater ease).

11. Although one-click notes and copy and paste features function differently, they largely present the same problem in that they both increase the speed and ease of inserting false information into a medical record. One-click notes, as the name suggests, allow physicians to paste a pre-programmed examination note with just one-click. *See, e.g.*, Daniel Essin, *The Ethical Dilemma Created by EHRs*, PHYSICIANS PRAC. (June 18, 2012),

opportunities for fraud, health care policymakers must continue to improve strategies of delegation.

Analysis proceeds in two parts. Part I reviews extant measures to delegate review over the certification of HIT and the challenges this effort has faced. Part II analyzes the rocky journey of private fraud detection contractors as they do more to analyze the massive set of claims generated by Medicare and Medicaid providers. Finally, this Article concludes with a prediction: increasing pressures on contractors to fight waste, fraud, and abuse will in turn shape information technology certification systems. In other words, there will be centripetal demands for integration of clinical decision support, revenue cycle management, and fraud detection in IT systems. While this transition may take a decade or more, it is a logical outgrowth of convergent socio-technical and socio-legal trends in health care.

I. AUTHORIZED TESTING AND CERTIFICATION BODIES (ATCBS) FOR HEALTH INFORMATION TECHNOLOGY

A. The Concept of (and Rationale for) Certification

We are all familiar with the basics of licensing and certification. Before you drive, hunt, or fish in most places, you need a license. The idea of licensing (if not the name "license") also appears in diverse other regulatory contexts. For instance, particularly before the Dodd-Frank Act,[12] and even today to some extent, many people consider an AAA-rating on a security as a needed license for those who may purchase it.[13] New drugs need Food and Drug Administration ("FDA") approval before they can be sold.

---

http://www.physicianspractice.com/blog/content/article/1462168/2083374; Donald Simborg, *Promoting Electronic Health Record Adoption: Is It the Correct Focus?*, 15 J. AM. MED. INFORMATICS ASS'N 127, 128 (2008). Many message prompts go too far and actively increase the ease of committing health care fraud by specifically advising physicians what documentation is required to justify higher billing codes. Farzad Mostashari, a former National Coordinator for ONC, has recognized that prompts that suggest more documentation to reach a higher billing code "might be over the line." *See* Robert Lowes, *Federal EHR Office to Look at Overbilling Allegations*, MEDSCAPE (Oct. 19, 2012), http://www.medscape.com/viewarticle/772944.

12. Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, § 931, 124 Stat. 1376, 1872 (2010) (codified as amended at 15 U.S.C. § 78o-7 (2012)).

13. For an in-depth discussion of the significance of credit rating agencies, see generally TIMOTHY J. SINCLAIR, THE NEW MASTERS OF CAPITAL: AMERICAN BOND RATING AGENCIES AND THE POLITICS OF CREDITWORTHINESS (2005). For creative proposals to formalize licensing of financial services, see Saule T. Omarova, *License to Deal: Mandatory Approval of Complex Financial Products*, 90 WASH. U. L. REV. 63, 113–

There is a great deal of interest in expanding the licensing concept (or rationale) to new areas of social life. For example, Joseph Lorenzo Hall has articulated a proposal for a "license plate for drones," requiring a certain basic form of permission and accountability for objects flying in the airspace below 400 feet.[14] Saule T. Omarova has suggested that certain exotic financial products should get pre-approval before they can be sold—she and other finance scholars have called for an "FDA of Financial Markets."[15]

1. Purposes of Regulation

Licensing fulfills many purposes. At its most basic, it allows central authorities a chance to know "what's out there," and to classify it. I have called this form of classification "Linnaean Regulation," after the work of the famous taxonomist who gave genus and species names to flora and fauna.[16] While the spirit of the Paperwork Reduction Act[17] may be to reduce unnecessary governmental reporting requirements, such policy commitments can and should be trumped in areas where new technology creates new risks and dangers. Linnaean regulation can do a great deal to rationalize regulatory agendas and priorities, too. For instance, if the Federal Aviation Administration receives five million applications for licenses for drones, they should loom as a much larger priority for the agency to investigate and consider than if, say, it receives five hundred. Similarly, the job of the Office of Financial Research will be

---

40 (2012) (proposing a broader set of regulatory interventions, including something along the lines of the FDA/licensing model); Eric A. Posner & E. Glen Weyl, *An FDA for Financial Innovation: Applying the Insurable Interest Doctrine to Twenty-First-Century Financial Markets*, 107 NW. U. L. REV. 1307, 1316–17 (2013) (discussing the pre-recession trend to label even subprime securities as AAA in order to bolster their marketability).

14. *License Plates & Drone Information Requirements*, DRONES & AERIAL ROBOTICS CONF., https://droneconference.org/darc_session/license-plates-drone-information-requirements/ (last visited May 7, 2014) (internal quotation marks omitted) (discussing a session chaired by Joseph Lorenzo Hall).

15. Omarova, *supra* note 13, at 113–40; Posner & Weyl, *supra* note 13, at 1348–57. *But see* Todd Zywicki, *CFPB "Plain Vanilla" Through the Back Door*, VOLOKH CONSPIRACY (Sept. 12, 2013, 11:42 AM), http://www.volokh.com/2013/09/12/cfpb-plain-vanilla-back-door/ (discussing the "plain vanilla" proposal that Congress rejected as a part of Dodd-Frank's establishment of the Consumer Financial Protection Bureau).

16. Frank Pasquale, *Linnaean Regulation in Health Insurance and Information Technology*, CONCURRING OPINIONS (Jan. 22, 2011), http://www.concurringopinions.com/archives/2011/01/linnaean-regulation-in-health-insurance-and-information-technology.html (last visited May 7, 2014).

17. *See* Paperwork Reduction Act of 1980, Pub. L. No. 96-511, 94 Stat. 2812 (codified as amended at 44 U.S.C. §§ 3501–3520 (2006)).

much easier once Legal Entity Identifiers ("LEI") are established.[18] The LEIs will be a crucial tool for tracking down exactly what financial securities are on the market, who owns them, and who is subject to obligations based on them. Finally, the Foreign Account Tax Compliance Act ("FATCA") will play a crucial role in helping tax authorities keep track of taxable income.[19] Each of these initiatives is an important step in creating a basic foundation of knowledge and analytics for law enforcement.

Complex and interlocking technological systems also create needs for basic tracking of what components are entering into these systems. On the most basic level, consider the development of railroads: if Chicago firms are building tracks of one gauge, and Milwaukee firms are building those of another, there will be trouble when they try to meet. In the realm of HIT, interoperability is also a pressing concern.[20] If one specialty decides on using a kind of HIT that cannot "talk"—i.e., communicate information accurately—to others, it could lead to serious efficiency losses in the future.

2. Quality Regulation

Does a product actually do what it is billed as doing? That is a primary concern of quality regulators. While a market economy often turns first to word of mouth or private quality raters and rankers,[21] and then to implied warranties of merchantability and fitness for a

18. *See* 45 C.F.R. § 170.302(o) (2012) (requiring each EHR system to "[a]ssign a unique name and/or number for identifying and tracking user identity"). This requirement is reminiscent of the Office for Financial Research's ("OFR") Legal Entity Identifier ("LEI") rulemaking. *See* Statement on Legal Entity Identification for Financial Contracts, 75 Fed. Reg. 74,146, 74,147 (Nov. 30, 2010), *available at* http://www.gpo.gov/fdsys/pkg/FR-2010-11-30/pdf/2010-30018.pdf.

19. The Foreign Account Tax Compliance Act ("FATCA") was enacted in 2010 as part of the Hiring Incentives to Restore Employment Act. *See* Hiring Incentives to Restore Employment Act, Pub. L. No. 111-147, § 501, 124 Stat. 71, 97–106 (2010) (codified as amended at 26 U.S.C. §§ 1471–1474 (2012)).

20. *See generally* JOHN PALFREY & URS GASSER, INTEROP: THE PROMISE AND PERILS OF HIGHLY INTERCONNECTED SYSTEMS 193–210 (2012) (describing the American HIT system and opportunities for reform).

21. *See, e.g.*, Kristin Madison, *The Law and Policy of Health Care Quality Reporting*, 31 CAMPBELL L. REV. 215, 227–30 (2009) (criticizing the various types of rankings for health care providers); Ann Marie Marciarille, *"How's My Doctoring?" Patient Feedback's Role in Assessing Physician Quality*, 14 DEPAUL J. HEALTH CARE L. 361, 362 (2012) (describing the power of user-generated medical reviews on "Angie's List, Yelp, and specialty sites like RateMDs.com"); *id.* at 385–88 (reporting on the non-public databases of physician quality markers, including the National Practitioners Data Bank and the CMS's Physician Compare program).

particular purpose as a second line of defense, sometimes a product or service needs governmental approval or inspection.[22]

3. Safety Regulation

On a more ambitious level, we also turn to licensing if there are certain dangers that can be prevented predictably by an initial approval process and neither tort nor contract liability can reliably deter a level of damage we want to prevent. If, for instance, plain milk turns out to be chocolate, a customer can arrive at a store for a refund. If the action happens repeatedly, or on a mass scale, a class may sue. But if the milk is poisoned, the damage to health cannot easily be undone. It makes sense to regularly inspect milk-producing facilities to assure that basic safeguards of pasteurization are in place.

B. Classification, Quality, and Safety Assurance in Health Information Technology

All of the classic rationales for certification and licensing are in place in the case of HIT. In terms of classification, it is now clear that the HIT industry is diverse and fragmented and likely to remain so for the foreseeable future.[23] As the eminent legal analyst of HIT, Nicolas Terry, has observed, IT staff have been "seeking to support individual clinical units" and thus are often adopting "fragmented HIT 'solutions,' such as freestanding computerized physician order entry or basic EMRs [electronic medical records]."[24] Some may dream of a disruptive innovator like Apple or Google sweeping in and consolidating existing technologies.[25] But that future is a long way off—if it is coming at all. In the meantime, we are stuck with trying to make sense of multiple systems, which must be coordinated in some way if the full advantages of big data methods in health care are to be

22. As an example, the quality and safety of electronic cigarette cartridges currently are not regulated by the FDA although the Agency recently submitted proposals for guidance. *See New & Events*, U.S. FOOD & DRUG ADMIN., http://www.fda.gov/newsevents/publichealthfocus/ucm172906.htm (last updated Apr. 24, 2014). Until a final rule is in place, any manufacturer can create its own flavored cartridges and sell them to consumers without guaranteeing the safety or quality of the ingredients.

23. Nicolas P. Terry, *Information Technology's Failure to Disrupt Health Care*, 13 NEV. L.J. 722, 742 (2013).

24. *Id.*

25. *See* Donald W. Simborg, Don Eugene Detmer & Eta S. Berner, *The Wave has Finally Broken: Now What?*, 20 J. AM. MED. INFORMATICS ASS'N e21, e23 (2013) (stating that "[s]uch a difficult market environment clearly inhibits the entry of new approaches to" electronic health records because the limited number of vendors that actually control the market prevents innovation and entry by other players).

realized. Classification is the first step toward assuring rational policy in the area.[26]

In terms of quality, HIT is about as close to a "credence good" as one can come.[27] It is very hard to fully assess the functionality of software until after one has used it in a variety of settings. Moreover, security concerns may arise only after a long period of use and may need a constantly evolving set of responses. The ongoing relationship between IT vendor and health care provider is so fraught with opportunities for one-sided contracts and unactionable neglect that it has been satirized in a widely shared website.[28] Providers may not estimate the risk of vendor problems properly or may contract away vital rights.[29]

Just as in health care generally, the question of safety in health care technology is vital.[30] The safety worries about health *information* technology both overlap with and are distinct from worries about health technology generally. But as these systems are increasingly integrated, misfires in the informational sector become more dangerous in the realm of treatment delivery. To borrow a phrasing of William Gibson: we are witnessing an "ever[sion]" of health

26. *See* 42 U.S.C. § 300jj-11(c)(5) (2012) (giving the Office of the National Coordinator for HIT the responsibility to "keep or recognize a program ... for the voluntary certification of health information technology").

27. *See* George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q.J. ECON. 488, 500 (1970) (discussing economic models involving "trust" and uncertain quality); Kenneth J. Arrow, *Uncertainty and the Welfare Economics of Medical Care*, 53 AM. ECON. REV. 941, 947, 965–66 (1963) (discussing behaviors influenced by information inequality in a medical context); Michael R. Darby & Edi Karni, *Free Competition and the Optimal Amount of Fraud*, 16 J.L. & ECON. 67, 68–72 (1973) (exploring credence goods where quality cannot be evaluated through normal use but only at additional cost).

28. *Welcome to Extormity*, EXTORMITY, http://www.extormity.com/ (last visited May 7, 2014).

29. The federal government's HIT website recommends the weighing of numerous factors to ensure a clinical decision support system's ("CDS") efficacy, such as the measure of CDS satisfaction and usability, workflow impact, utilization, and unintended consequences. *Measure Effects and Refine CDS Interventions*, HEALTH IT, http://www.healthit.gov/sites/default/files/3-4-5-measure-effects-and-refine-cds-interv.pdf (last visited May 7, 2014).

30. *See* Walt Bogdanich & Kristina Rebelo, *A Pinpoint Beam Strays Invisibly, Harming Instead of Healing*, N.Y. TIMES, Dec. 29, 2010, at A1 (highlighting how medical devices that require pinpoint accuracy can cause great damage to patients when set up incorrectly); Nicolas P. Terry, *When the Machine That Goes Ping Causes Harm*, 46 ST. LOUIS U. L.J. 37, 58–59 (2002) (noting that the medical professional-centered tort liability system currently governing health care improperly "permit[s] health care entities to shift costs associated with ameliorating technologies" to patients).

information technology, an increasingly seamless integration of their digital forms into the fabric of everyday treatment decisions.[31]

C. *The Current Landscape of Health Information Technology Certification and Licensing*

An Electronic Health Record ("EHR") is defined by statute as "an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff."[32] Since the second Bush administration, health policymakers have been focused on getting more providers to use digital medical record systems.[33] The critical legislative step toward realizing that goal was the Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH").[34] HITECH established the first subsidies for those providers *meaningfully* using health records.[35] By 2016, those subsidies will convert to penalties for Medicare reimbursements of those *not* using EHRs; the carrot turns into a stick.[36] The idea here was to prevent providers from simply, say, putting a transcript of a patient visit into Microsoft Word, calling that process "adoption of EHR," and getting subsidies for it. About thirty-five billion dollars in subsidies were appropriated for this purpose.[37]

The rationale here was that, once medical records were fully computerized in systems with a rich set of functionalities and interoperability capabilities, savings would follow and quality of care

---

31. William Gibson, *Google's Earth*, N.Y. TIMES, Sept. 1, 2010, at A23.

32. 42 U.S.C. § 17921(5) (2012).

33. *See* Nicolas P. Terry, *Anticipating Stage Two: Assessing the Development of Meaningful Use and EMR Deployment*, 21 ANNALS HEALTH L. 103, 103 (2012). *See generally* Catherine M. DesRoches et al., *Electronic Health Records in Ambulatory Care: A National Survey of Physicians*, 359 NEW ENG. J. MED. 50 (2008) (studying the use of EHRs in ambulatory care); Ashish K. Jha et al., *Use of Electronic Health Records in U.S. Hospitals*, 360 NEW ENG. J. MED. 1628 (2009) (studying the use of EHRs in U.S. hospitals).

34. American Recovery and Reinvestment Act of 2009 ("ARRA"), Pub. L. 111-5, 123 Stat. 115 (2009) (codified in scattered sections of the U.S.C.). For further discussion of meaningful use, see Mark Faccenda & Lara Parkin, *Meaningful Use—What Does It Mean to You?*, 23 HEALTH L. 10, 10 (2011) (citing the ARRA).

35. *See* Bob Brown, *What Is a "Certified EHR"?*, 12 J. HEALTH CARE COMPLIANCE 31, 31 (2010); Nicolas P. Terry, *Certification and Meaningful Use: Reframing Adoption of Electronic Records as a Quality Imperative*, 8 IND. HEALTH L. REV. 43, 46 (2011).

36. Terry, *supra* note 35, at 50.

37. Rob Girling, *The Elusive Promise of Electronic Health Records*, MEDCITYNEWS (Jan. 20, 2014, 1:00 PM), http://medcitynews.com/2014/01/elusive-promise-electronic-health-records/.

would improve.[38] The law is designed to do more than subsidize; it conditions funding on the "meaningful use" of electronic medical records.[39] "Meaningful use" regulations define how functional an EHR system has to be before its user can receive subsidies.[40] Over a six-year period, these regulations will be implemented in three stages.[41] Their purpose is to incentivize improvements to quality, safety, efficiency, and care coordination; engage patients and families; and improve population health—all while protecting privacy, confidentiality, and security.[42] As such, EHRs must at least include basic information such as patient demographics, clinical health information, and medical history.[43]

The HITECH Act also mandates that the Department of Health and Human Services ("DHHS") establish procedures for certifying HIT so that providers can be assured that their technology meets basic standards.[44] Self-regulation would not adequately vindicate the interests of all stakeholders.[45] To ensure optimal data use, basic

38. A meta-study concluded that ninety-two percent of recent articles on HIT did find positive benefits overall. *See* Melinda Beeuwkes Buntin et al., *The Benefits of Health Information Technology: A Review of the Recent Literature Shows Predominantly Positive Results*, 30 HEALTH AFF. 464, 466–67 (2011).

39. *See* Camella B. Boateng, *Federal Electronic Health Records Incentive Programs: What They Mean for Compliance Officers*, 12 J. HEALTH CARE COMPLIANCE 17, 18 (2010) ("The meaningful use objectives are divided into two groups: (1) core set and (2) menu set objectives. The core set contains 14 required objectives that eligible hospitals must fulfill to receive bonus payments. The menu set has 10 objectives, and hospitals must select and meet five objectives for payment purposes.").

40. *See* David Blumenthal & Marilyn Tavenner, *The "Meaningful Use" Regulation for Electronic Health Records*, 363 NEW ENG. J. MED. 501, 501 (2010).

41. *See* Medicare and Medicaid Programs, 75 Fed. Reg. 44,314, 44,328 (proposed July 28, 2010) (codified at 42 C.F.R. pts. 412, 413, 422) (listing the "core set of meaningful use objectives" for Stage 1). Capabilities include: recording smoking status and body mass index; presenting clinical data on individual patients, including medication list, medication allergy list, problem and current diagnosis list, and a clinical summary; generating lists of patients by specific condition and allowing communication with patients for reminders and such; allowing patients timely access to their EHR; and allowing providers to submit claims for payment and information to public health authorities electronically. *Id.*

42. Nicolas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 U. ILL. L. REV. 681, 691–96 (2007).

43. 42 U.S.C. § 300jj(13) (2012).

44. *See* Health Information Technology Standards, 45 C.F.R. § 170 (2013); Proposed Establishment of Certification Programs for Health Information Technology, 75 Fed. Reg. 11,328 (proposed Mar. 10, 2010) (to be codified at 45 C.F.R. pt. 170); Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 75 Fed. Reg. 44,590 (proposed July 28, 2010) (to be codified at 45 C.F.R. pt. 170).

45. *See* Melissa M. Goldstein & Jane Hyatt Thorpe, *The First Anniversary of the Health Information Technology for Economic and Clinical Health (HITECH) Act: The Regulatory Outlook for Implementation*, 7 PERSPECTIVES HEALTH INFO. MGMT. 1, 4

benchmarks for data entry and portability are needed. Certified EHRs must include capacities that "enable providers to achieve meaningful use as it is currently constituted in Phase 1 of HHS' regulations."[46] The Office of the National Coordinator for Health Information Technology ("ONC")[47] delegates certification authority to Authorized Testing and Certification Bodies ("ATCBs" or "ACBs"), which will follow standards developed by the International Organization for Standardization.[48]

The meaningful use and certification standards are a comprehensive, complex effort to create rules and standards that can support a twenty-first century HIT infrastructure. This effort heavily depended on cooperation between public and private partners.[49] The chain of certifications between DHHS and HIT vendors essentially extends via the National Institute of Standards and Technology ("NIST") to the ATCBs.[50] There are currently six approved ATCBs, and all were approved in 2010.[51] There are six accredited testing laboratories.[52] The same company can be both a certification body

(2010) (arguing that EHR technology previously certified by the Certification Commission for Healthcare Information Technology ("CCHIT") before the ARRA was "difficult to use . . . and [was] not designed to meet ARRA's goals of improving quality and efficiency in the healthcare system").

46. Sharona Hoffman & Andy Podgurski, *Meaningful Use and Certification of Health Information Technology: What About Safety?*, 39 J.L. MED. & ETHICS S77, S78 (2012) [hereinafter *Meaningful Use*]; *see* Sharona Hoffman & Andy Podgurski, *Finding a Cure: The Case for Regulation and Oversight of Electronic Health Record Systems*, 22 HARV. J.L. & TECH. 103, 146 (2008) (claiming that a committee of practitioners, rather than "HIT industry personnel," would be more "likely to prioritize the best interests of practitioners and patients over the interests of industry and thus to subject EHR systems to rigorous evaluation," but not directly criticizing ATCBs, which had not been certified at this point in time).

47. The ONC is organizationally located within DHHS and "is the principal federal entity charged with coordination of nationwide efforts to implement and use the most advanced health information technology and the electronic exchange of health information." *About ONC*, HEALTH IT, httphttp://www.healthit.gov/newsroom/about-onc (last visited May 7, 2014).

48. Principles of Proper Conduct for ONC-ATCBs, 45 C.F.R. § 170.423 (2013).

49. Public-private partnerships are necessary to the prevention of health care fraud more generally. *See Public-Private Partnership to Prevent Health Care Fraud*, STOP MEDICARE FRAUD, http://www.stopmedicarefraud.gov/aboutfraud/public-private/index.html (last visited May 7, 2014).

50. Permanent Certification Program for HIT, 45 C.F.R. §§ 170.500–170.599 (2013).

51. *Certification Programs & Policy: Authorized Testing and Certification Bodies*, HEALTH IT, http://www.healthit.gov/policy-researchers-implementers/authorized-testing-and-certifications-bodies (last visited May 7, 2014).

52. *Directory of Accredited Laboratories: Healthcare Information Technology Testing*, NAT. VOLUNTARY LAB. ACCREDITATION PROGRAM, http://ts.nist.gov/standards/scopes/hit.htm (last visited May 7, 2014).

and a laboratory as long as there is a "strong firewall between the two programs."[53]

Nevertheless, critical voices still question whether the certification standards (and those implementing them) are optimal. For instance, they may not be adequately tailored to the diverse specialties in medicine.[54] Small providers also may want to seek special allowances or tailored programs.[55] Diversity of regions also may not be taken into account; one can imagine, for instance, that the competitive landscape of providers is much different in, say, Boca Raton, Florida, than Billings, Montana.[56] Like some of the small groups or individual policyholders who had their policies cancelled in the wake of implementation of many aspects of ACA insurance regulation, these small providers may feel that federal guidance is unduly Procrustean.[57]

Physicians have complained that administrators focus too much on profitability and return on investment, and minimize the input of frontline providers who may want more functionalities or safeguards.[58] Moreover, ongoing security and maintenance concerns

53. *Getting Started with Certification: Certification Bodies & Testing Laboratories*, HEALTH IT, http://www.healthit.gov/policy-researchers-implementers/certification-bodies-testing-laboratories (last visited May 7, 2014).

54. *See* Robert S. Miller, *Electronic Health Record Certification in Oncology: Role of the Certification Commission for Health Information Technology*, 7 J. ONCOLOGY PRAC. 209, 210–11 (2011) (explaining that the "CCHIT Certified program is voluntary and its testing criteria are created by experts with domain and specialty expertise, whereas ONC-ATCB certification is mandated by the federal government for those wishing to collect meaningful use incentive dollars, with criteria established in published government rules" and later referring to the CCHIT program as "robust").

55. *See* Sowmya R. Rao et al., *Electronic Health Records in Small Physician Practices: Availability, Use, and Perceived Benefits*, 18 J. AM. MED. INFORMATICS ASS'N 271, 275 (2011) (criticizing the certification program for failing to take notice of the special challenges facing small providers).

56. *See, e.g.*, Joshua R. Vest, Jangho Yoon & Brian H. Bossak, *Changes to the Electronic Health Records Market in Light of Health Information Technology Certification and Meaningful Use*, 20 J. AM. MED. INFORMATICS ASS'N 227, 231 (2013) (arguing for "targeted" HIT policies regarding certification because vendor competition varies geographically).

57. Regarding the position of policyholders impacted by ACA regulation implementation, see *Actually, You Can't "Keep It,"* ON THE MEDIA (Nov. 1, 2013), http://www.onthemedia.org/story/actually-you-cant-keep-it/transcript/# (noting 9 million potentially cancelled insurance policies and occasional cases of discontent).

58. *See* Simborg, Detmer & Berner, *supra* note 25, at e22 (explaining that physicians who use EHR continue to report dissatisfaction with the usability and interface). The authors attribute the dissatisfaction to the different nature of EHR, as compared to other consumer programs, because EHR systems are typically purchased by administrators, who are focused on profitability and return on investment. As such, vendors have focused on these traits, and physician input may be minimized. *Id.* The authors also cite market dynamics as a reason EHR has not reached its full potential because five EHR vendors

cannot be addressed in a single, one-off licensing.[59] Renewal of certification may be an important aspect of future regulatory structures. Moreover, ATCBs (or other entities) ought to be more open to assessing the ongoing performance of vendors.[60] By adopting relatively easy-to-understand ranking and rating systems, they could help avoid the classic "lemons market" problem by translating performance on a variety of metrics into a relatively straightforward assessment of the comparative merits of various vendors.

There are also price levels among ATCBs that deserve further investigation.[61] DHHS has declined "to dictate the minimum or maximum amount an ONC–ACB should be able to charge for certifying a Complete EHR or EHR Module," relying instead on a competitive market of "multiple ONC–ACBs" to reduce costs.[62] DHHS also has stated that additional regulatory controls are unnecessary because ONC-ACBs must "comply with Guide 65, which requires certification bodies to make their services accessible to all applicants whose activities fall within its declared field of operation

---

account for fifty percent of the market share. *Id.* at e23 ("Such a dif•cult market environment clearly inhibits the entry of new approaches to EHR." (citing Joseph Goedert, *Research Tracks Physician I.T. Adoption in 2012*, HEALTH DATA MGMT. (Sept. 28, 2012), http://www.healthdatamanagement.com/ad_includes/welcome.html)).

59. *See* Hardeep Singh, David C. Classen & Dean F. Sittig, *Creating an Oversight Infrastructure for Electronic Health Record-Related Patient Safety Hazards*, 7 J. PATIENT SAFETY 169, 169 (2011) ("[ATCB certification] does not guarantee that EHRs will actually be implemented and work as planned; therefore, ongoing system evaluations and modifications are necessary. At present, it is unclear which single agency is responsible for EHR oversight.").

60. *See* Amanda Parsons & Winfred Wu, *In Response To: Electronic Health Records in Small Physician Practices: Availability, Use, and Perceived Benefits*, 18 J. AM. MED. INFORMATICS ASS'N 726, 726 (2011) (advocating for organizations to assist small providers in their use of EHR and claiming that "EHR certification programs like ONC ATCB should take into account vendor performance and user reviews, as well as ensuring that vendors have correctly coded key functionality, like measures of clinical quality and meaningful use metrics").

61. Stephen Barlas, *Hospitals Scramble to Meet Deadlines for Adopting Electronic Health Records: Pharmacy Systems Will Be Updated Slowly but Surely*, 36 PHARMACY & THERAPEUTICS 37, 40 (2011) (describing the different prices between ACTBs as a "thorny issue" and explaining that "CCHIT charges vendors more for certifying [for multiple uses, including non-HITECH criteria,] a full EHR system compared with Drummond, which charges $19,000; InfoGard's price is $19,400").

62. Establishment of the Permanent Certification for Health Information Technology, 76 Fed. Reg. 1262, 1314 (Jan. 7, 2011); *see id.* at 1279 ("[T]he actual costs of testing and certification may be lower than our estimates due to factors such as competitive pricing and/or lower costs attributable to gap certification."); *id.* at 1307 ("Aside from the requirements discussed above, we do not specify the fees or any other processes that an ONC–ACB must follow before granting certified status to a newer version of a previously certified Complete EHR or EHR Module based on the submitted attestation.").

. . . , including not having any undue financial or other conditions."[63] But there is justifiable worry that there may eventually be price competition that could erode the ability of the certification bodies to improve their analysis and tempt them to lower standards.

Critics also go beyond complaining about ATCBs to a focus on ONC itself.[64] Joseph Conn has argued that "the five ONC-approved independent testing and certification bodies can't do their jobs because several essential testing 'tools'—custom-made software programs government contractors developed for the ONC—have not been completely debugged."[65] For example, Conn notes as follows:

> On Jan. 23, Carol Bean, director of the ONC's certification office, sent a memo to the testing and certification bodies, acknowledging problems with a different tool, the program's Transport Test Tool. That tool, developed for ONC with help from the National Institute of Standards and Technology, is designed to test EHRs on Stage 2 requirements for exchange of patient-care summaries and other secure messages, important first steps under the program in a long march toward EHR interoperability.[66]

Repeated delays in the implementation of more advanced International Classification of Diseases nomenclature have also created some uncertainty and frustration among vendors and providers—though the ONC would certainly have provoked even more uncertainty and frustration had it simply barreled ahead with the plan to move from roughly 14,000 to over 140,000 categories.[67] These problems give some ammunition to those who would shift toward a more privatized model of EHR quality maintenance.[68]

---

63. *Id.* at 1309; *see id.* at 1268 (citing *ISO/IEC Guide 65:1996*, INT'L ORG. FOR STANDARDIZATION). Guide 65 is incorporated into the code at 42 C.F.R. § 170.599(b)(2).

64. Joseph Conn, *Certified Trouble: Vendors Wait for Feds to Debug EHR Testing Tools*, MODERN HEALTHCARE, Jan. 28, 2013, at 12–13 (detailing the problems developers have had getting software approved for the 2014 Stage 2 requirements because the ONC has not provided the certification bodies with properly functioning testing programs).

65. *Id.*

66. *Id.*

67. *See* Joseph Conn, *Riding the Wave: As Federal EHR Incentives Recede, the Next Surge in Health IT Spending Begins to Take Shape*, MODERN HEALTHCARE, May 20, 2013, at 7 (citing sources that believe " 'EHRs have peaked,' . . . but it doesn't follow that overall healthcare IT sales will be dragged down"). Other potential sources of HIT spending include the government-mandated conversion to ICD-10 billing. *Id.*

68. *See, e.g.*, Jonathon H. Roth, Note, *Regulating Your Medical History without Regulations: A Private Regulatory Framework to Electronic Health Record Adoption*, 91 B.U. L. REV. 2103, 2118–20 (2011).

Nevertheless, given the critical functionalities involved, there must be some public mandates for baseline levels of quality assurance. There is an ongoing need for public-private partnership: most of the relevant infrastructure will always be in private hands, but its owners do not have adequate incentives to maximize or even optimize outcomes. For example, we might rely on the tort system to deter gross failures in record systems. Certainly a jury would be sympathetic to claims resulting from a foreseeable meltdown of a system.[69] But what of the thousands or even millions of people who might benefit from careful and comprehensive data collection that would enable data analysis that could in turn lead to far better treatment repertoires?

In 2011, EHR experts Sharona Hoffman and Andy Podgurski sounded another note of alarm about the development of digitized health infrastructure.[70] They argued that early rounds of regulations relating to HIT failed to address safety concerns. "General system safety is a property that is attainable only through rigorous processes for development and evaluation," they noted, but they felt that the CCHIT was not capable of providing such processes.[71] It still remains to be seen whether ATCBs are up to this task.

II. CMS'S FRAUD-DETECTION CONTRACTORS

In any large government program, there always are a few bad apples looking to exploit the system.[72] The question for CMS was how to guard the American taxpayers' funds as some of the largest government programs on the planet disbursed funds to hundreds of thousands of entities.[73] Given the sheer volume and complexity of the transactions involved, and broader neoliberal resistance to

69. Of course, we should not be too reliant on the tort system either. EHR failures are potentially opportunities for multiple parties to shift blame among one another, obscuring causation and making it very difficult to find out exactly who was responsible for any given error.

70. Hoffman and Podgurski anticipated these concerns in 2009. *See* Sharona Hoffman & Andy Podgurski, *E-Health Hazards: Provider Liability and Electronic Health Record Systems*, 24 BERKELEY TECH. L.J. 1523, 1527 (2009); *Meaningful Use*, *supra* note 46, at S78.

71. *See Meaningful Use*, *supra* note 46, at S78.

72. *See* Lewis Morris & Gary W. Thompson, *Reflections on the Government's Stick and Carrot Approach to Fighting Health Care Fraud*, 51 ALA. L. REV. 319, 322 (1999) (providing that, while the public may believe health care fraud to be widespread, "government spokespersons have continuously acknowledged that most providers deal with the federal health care programs in an honest and ethical manner").

73. *See id.* at 321 (highlighting government audits that suggested more than $20 billion a year in Medicare overpayments were made in the mid-1990s).

government hiring, CMS had little choice but to involve contractors to detect and deter fraud.[74]

The same technological and legal revolutions that have eviscerated personal privacy are starting to transform law enforcement.[75] Directed at the right targets, data mining and pervasive surveillance can advance our understanding of the social world, and they might even prevent the types of massive misallocations of resources that have led to "triple fails" in the U.S. health care system: unnecessary spending that does nothing to improve outcomes but also manages to reduce access to the system.[76]

There are many routes to fraud and abuse in the programs.[77] Examples of Medicare fraud include as follows:

> Billing for services that [a physician] did not actually render; [b]illing for services that were not medically necessary; [b]illing for services that were performed by an improperly or unsupervised employee; [b]illing for services that were performed by an employee who has been excluded from participation in Federal Health Care programs; [b]illing for services of such low quality that they are virtually worthless; and [b]illing separately for services already included in a global fee . . . .[78]

Medicare abuse results from activities that unnecessarily increase costs to Medicare and involve practices that are not in the best interest of patient care or that are not medically necessary.[79] According to one estimate by fraud examiners, about $133 billion of

---

74. *See* REBECCA SALTIEL BUSCH, HEALTHCARE FRAUD: AUDITING AND DETECTION GUIDE 14–15 (2d ed. 2012).

75. *See* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE HIDDEN ALGORITHMS BEHIND MONEY AND INFORMATION ch. 5 (forthcoming 2014).

76. For a definition of "triple fail" events, see Geraint Lewis et al., *How Health Systems Could Avert "Triple Fail" Events That Are Harmful, Are Costly, and Result in Poor Patient Satisfaction*, 32 HEALTH AFF. 669, 669–70 (2013).

77. *See, e.g.*, MALCOLM K. SPARROW, LICENSE TO STEAL: HOW FRAUD BLEEDS AMERICA'S HEALTH CARE SYSTEM 40 (2000) (discussing one way in which perpetrators of health care fraud can find, and then exploit, weaknesses in claims payment systems).

78. CTRS. FOR MEDICARE & MEDICAID SERVS., DEP'T OF HEALTH & HUMAN SERVS., MEDICARE FRAUD & ABUSE: PREVENTION, DETECTION AND REPORTING 6 (2012), *available at* http://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/downloads/Fraud_and_Abuse.pdf. This document also mentions "[m]isusing codes on a claim, [c]harging excessively for services or supplies, and [b]illing for services that were not medically necessary." *Id.* at 2.

79. *Id.*; *see also, e.g.*, Reed Abelson & Julie Creswell, *A Hospital Chain's Inquiry Cited Unneeded Treatment*, N.Y. TIMES, Aug. 7, 2012, at A1 (discussing allegations that a hospital was performing unnecessary procedures on patients).

all payments by CMS in 2008 were distributed improperly due to the filing of illegitimate claims.[80]

CMS uses private contractors to process Medicare claims and investigate fraud perpetrated by providers, beneficiaries, and third-parties.[81] For many purposes, including routine claims processing and audits, such entities are entirely qualified to exercise judgment, catch errors, and educate providers on how to avoid such errors in the future.[82] However, as they have shouldered more responsibilities, these contractors are facing opposition.[83] Their internal processes can be obscure. Providers often feel confused and frustrated.[84] A critical mass of complaints indicates that the deputization of important powers to private contractors in the areas of fraud investigation and payment recoupment needs better supervision.[85]

---

80. Jeffrey R. Helton, *Avoiding Fraud Risks Associated with EHRs*, HEALTH FIN. MGMT., July 2010, at 76, 78.

81. *See* CTRS. FOR MEDICARE & MEDICAID SERVS, PUB. NO. 100-08, MEDICARE PROGRAM INTEGRITY MANUAL §§ 1.1–1.3, *available at* http://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Internet-Only-Manuals-IOMs-Items/CMS019033.html (describing CMS contractors and their tasks); *see also id.* §§ 4.1–4.2 (describing Medicare fraud and fraud investigation).

82. CTRS. FOR MEDICARE & MEDICAID SERVS, IMPROPER MEDICARE FEE-FOR-SERVICE PAYMENTS REPORT NOVEMBER 2009 1, 23 (2009), *available at* http://www.cms.gov/CERT/Downloads/CERT_Report.pdf.

83. AM. MED. ASS'N, MEDICARE AND MEDICAID PROGRAM INTEGRITY: RECOMMENDATIONS FOR GREATER VALUE AND EFFICIENCY 2 (2012), *available at* http://www.ama-assn.org/resources/doc/washington/medicare-medicaid-program-integrity.pdf; Dani Grigg, *Medical Suppliers in Idaho and Nationwide Scramble to Keep Up with Surging Medicare Audits*, IDAHO BUS. REV., June 29, 2012 (describing provider and supplier disenchantment).

84. AM. MED. ASS'N, *supra* note 83, at 2 ("MACs have discretion to require an unlimited number of medical records. And, while the Medicare RACs have similar appeals processes to the MACs, each Medicaid RAC may have a different appeals process. Consequently, physicians spend a great deal of time determining which contractor is auditing them, under what authority, and what the guidelines are for response. This confusion and misspent time unduly burdens physicians and contravenes the swift recoupment of improper payments to the federal government .... [Thus] CMS has committed to undertake an 'Audit of Audits' to review the myriad federal audit contractors and identify areas of duplication.").

85. *See* Letter from Sens. Max Baucus, Orrin G. Hatch, Ron Wyden, Tom Coburn, Tom Carper, & Charles E. Grassley to Members of the Health Care Community (May 2, 2012), *available at* http://www.finance.senate.gov/newsroom/ranking/download/?id=85cc3a87-5714-4d93-8cf1-0a338a33083a (requesting ideas from medical professionals regarding how to best combat issues of health care fraud and waste).

A. *Background on Fraud Investigations*

Fraud investigations in the Medicare and the Medicaid programs have evolved over time.[86] The Medicare Prescription Drug, Improvement, and Modernization Act of 2003[87] ("MMA") authorized CMS to replace Fiscal Intermediaries ("FIs") with Medicare Administrative Contractors ("MACs")[88] and to replace Program Safety Contractors ("PSCs") with Zone Program Integrity Contractors ("ZPICs").[89] Recovery Auditors ("RAs," formerly "RACs," Recovery Audit Contractors) have been in development since the MMA, but the program was officially mandated after the Tax Relief and Health Care Act of 2006.[90] The Comprehensive Error Rate Testing program ("CERT") was established after the Improper Payments Information Act of 2002.[91]

Fraud prevention and investigation begins when a provider submits a claim to a MAC or when an individual submits a complaint to either the Beneficiary Contact Center or to any other agency equipped to receive fraud complaints.[92] The MAC reviews claims for abnormal activity based on identified vulnerabilities and tries to resolve them.[93] It also receives complaints that cannot be resolved.[94] If the MAC finds evidence of fraud, it refers the claim to the ZPIC, which investigates further.[95] The ZPIC can also refer the case to law enforcement for civil or criminal investigation.[96] RAs conduct extensive post-payment reviews of claims in order to identify and

86. *See, e.g.*, OFFICE OF THE INSPECTOR GEN., DEP'T OF HEALTH & HUMAN SERVS., OEI-04-11-00101, VULNERABILITIES IN CMS'S AND CONTRACTORS' ACTIVITIES TO DETECT AND DETER FRAUD IN COMMUNITY MENTAL HEALTH CENTERS 6 n.27, 8 n.45 (2013) (explaining that not all legacy contractors had been replaced).

87. Pub. L. No. 108-173, 117 Stat. 2066 (codified as amended in scattered sections of 42 U.S.C.).

88. OFFICE OF THE INSPECTOR GEN., *supra* note 86, at 5.

89. *Id.* at 7–8.

90. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-522, MEDICARE PROGRAM INTEGRITY: INCREASING CONSISTENCY OF CONTRACTOR REQUIREMENTS MAY IMPROVE ADMINISTRATIVE EFFICIENCY 10–11 (2013); Tax Relief and Health Care Act of 2006, Pub. L. No. 109-432, 120 Stat. 2922 (codified in scattered sections of 26 U.S.C.).

91. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 90, at 11; Improper Payments Information Act of 2002, Pub. L. 107-300, 116 Stat. 2350. CERT is responsible for calculating MAC improper payment rates. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 90, at 15 tbl. 2. Although CERT conducts activities related to fraud prevention, such as identifying vulnerabilities, CERT refers improper payments to the MAC. *Id.* at 19.

92. *See generally* CTRS. FOR MEDICARE & MEDICAID SERVS., *supra* note 81, § 4 (describing the benefit integrity program).

93. *Id.* §§ 2.1–2.2.

94. *Id.*

95. *Id.* § 4.2.

96. *Id.* § 4.18.1.

recoup improper payments.[97] MACs process the overpayments RAs identify and conduct the appeals process.[98]

MACs have primary responsibility to prevent and investigate Medicare fraud. They can prevent payments to providers.[99] ZPICs also investigate suspected cases of fraud.[100] Both types of contractors have access to extensive data and the capabilities to analyze it.[101] ZPICs use internal data analysis to prevent and detect fraud.[102]

Given the ubiquity of cameras, sensors, and "guard labor,"[103] advanced industrial societies have opportunities to prevent crime in the twenty-first century that may have been considered "science fiction" in the twentieth.[104] Professor Michael Rich has even recently asked, "Should we make crime impossible?"[105] The stakes of pervasive, constant, data-driven surveillance are high. As Evgeny Morozov observed recently, systems like PredPol[106] have been used by police forces to predict with sometimes uncanny accuracy the likelihood of crime happening in a given area.[107] Digital environments for health care claim entry should, in principle, be even more susceptible to a "panoptic sort"—an all-seeing aggregation of

97. *See generally* CTRS. FOR MEDICARE & MEDICAID SERVS., PUB. NO. 100-06, FINANCIAL MANAGEMENT MANUAL §§ 100.1-100.15 (2013), *available at* http://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Downloads/fin106c04.pdf (providing further information on the functions of Recovery Auditors).

98. *Id.* § 100.5.

99. CTRS. FOR MEDICARE & MEDICAID SERVS., *supra* note 81, § 3.7.

100. *Id.* § 4.2.

101. *See generally id.* § 2 (describing the types of data and analysis).

102. *See* Sara Kay Wheeler, Stephanie L. Fuller & J. Austin Broussard, *Meet the Fraud Busters: Program Safeguard Contractors and Zone Program Integrity Contractors*, 4 J. HEALTH & LIFE SCI. L. 1, 15–16 (describing data analysis responsibilities of PSCs and ZPICs).

103. *See generally* Arjun Jayadev & Samuel Bowles, *Guard Labor*, 79 J. DEV. ECON. 238 (2006) (defining "guard labor").

104. *See* James Byrne & Gary Marx, *Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact*, J. POLICE STUDIES, Sept. 2011, at 17, 22–25 (discussing crime prevention innovations including risk classification tools and protections for data privacy).

105. Michael L. Rich, *Should We Make Crime Impossible?*, 36 HARV. J.L. & PUB. POL'Y 795, 796 (2013) (discussing " 'impossibility structures,' government mandates that aim to make certain classes of criminal conduct effectively impossible" (footnote omitted)).

106. PredPol is a computer system that analyzes data on past crime patterns to predict where and when future law-breaking will occur. *See About*, PREDPOL, http://www.predpol.com/about/ (last visited May 7, 2014)

107. EVGENY MOROZOV, TO SAVE EVERYTHING, CLICK HERE: THE FOLLY OF TECHNOLOGICAL SOLUTIONISM 250 (2013).

multiple data sources designed to identify troubling behavior.[108] That was one central motivating factor behind the extensive delegations of investigative authority to fraud contractors, acquiesced to by providers themselves as part of Medicare Conditions on Participation.[109]

The effort got off to a rocky start. PSCs did not make adequate use of proactive fraud prevention and investigation techniques like data analysis.[110] CMS's oversight of both PSCs and ZPICs left something to be desired, suggesting a larger problem in excess outsourcing and contracting out: the declining ability of the government to monitor and control the sprawling array of contractors that it has created.[111] The overarching issue is that a federal government that has become so reliant on contractors may be losing its ability to assess the functionality and value of contractors' handiwork.[112]

For example, the mandated transfer of responsibilities from PSCs to ZPICs was fraught with difficulties. While ZPICs were supposed to rely on data analysis, their work remained, like the PSCs, driven more by beneficiary complaints.[113] External sources of information, such as beneficiary complaints, can be less reliable and more scattershot than internal data analysis.[114] The hope for advocates of data-driven fraud prevention and investigation is that the detection of problematic behavior can become more systematic

108. *See* David Lyon, *Surveillance as Social Sorting: Computer Codes and Mobile Bodies*, *in* SURVEILLANCE AS SOCIAL SORTING: PRIVACY, RISK, AND DIGITAL DISCRIMINATION 20 (David Lyon ed., 2003) (discussing the role of searchable databases in everyday surveillance and the use of such tools in classifying individuals and groups). The term "panoptic sort" comes from the work of Oscar Gandy. *See* OSCAR H. GANDY, THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION 15 (1993).

109. *See* Wheeler, Fuller & Broussard, *supra* note 102 ("PSCs and ZPICs are expected to engage in proactive and comprehensive data analysis to identify actual or potential claim payment errors and potential fraud.").

110. *See* Memorandum from the Inspector Gen. to the Sec'y of DHHS, Top Management and Performance Challenges Facing the Department of Health and Human Services in Fiscal Year 2011 (Nov. 10, 2011), *available at* http://oig.hhs.gov/reports-and-publications/top-challenges/2011/2011-tcm.pdf.

111. *See* FREEMAN & MINOW, *supra* note 8, at 3. *See generally* PAUL R. VERKUIL, OUTSOURCING SOVEREIGNTY 1–6 (2007) (discussing the tension between efficiency and accountability when governmental tasks are outsourced to private entities).

112. *See* FREEMAN & MINOW, *supra* note 8, at 3; Pierce, *supra* note 8, at 1218.

113. OFFICE OF INSPECTOR GEN., DEP'T OF HEALTH & HUMAN SERVS., OEI-04-11-00220, CMS AND CONTRACTOR OVERSIGHT OF HOME HEALTH AGENCIES 16 (2012) (noting that "investigations of 192 of 255 (75 percent) [Home Health Agencies] were initiated from external sources. . . . [such as] beneficiary complaints").

114. *Id.* CMS responded that the agency will be updating its analytical models and the statement of work for ZPICs. *Id.* at 21.

once a large enough dataset has established the predicates for troubling behavior.

To understand how this might work (and the relevance of automated pattern-recognition to law enforcement generally), consider recent reporting on Target's use of data.[115] The massive retailer prides itself on knowing a great deal about its customers—including whether they are pregnant.[116] The pattern recognition was relatively easy. First, Target's statisticians compiled a database of "the known pregnant"—people who had signed up for its baby registries.[117] They then compared the purchases in that dataset to the purchases made by Target shoppers as a whole.[118] By analyzing where the pregnant shoppers diverged the most from the general dataset, they could find various "signals" of pregnancy-related purchases.[119] In the first twenty weeks, "supplements like calcium, magnesium and zinc" were a tip-off.[120] Later in the pregnancy, "scent-free soap and extra-big bags of cotton balls" were common purchases.[121] By the end of the analysis, statisticians compiled a list of twenty-five products that contributed to a "pregnancy prediction score" and due date estimator.[122] For example, if a twenty-three year old woman in Atlanta bought "cocoa-butter lotion, a purse large enough to double as a diaper bag, zinc and magnesium supplements and a bright blue rug" in March, Target estimated an eighty-seven percent chance she is pregnant and due to give birth in late August.[123]

Now consider the application of the same methods in the fraud and abuse context. CMS already has access to a critical mass of complaints regarding fraudulent contractors and to digitized records of their past patterns of filing claims for reimbursement.[124] A

115. *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all&_r=2&.

116. *Id.*

117. *Id.*

118. *Id.* (explaining that every Target shopper has a "Guest ID" number, tied to a credit card, email address, or other identifier).

119. *Id.*

120. *Id.*

121. *Id.*

122. *Id.*

123. *Id.* In at least one case, the company mailed coupons for pregnancy-related items to the house of a teen who had not yet told her father she was pregnant. When other customers found the pregnancy-related ads creepy, Target responded—not by explaining its data collection to customers, but by mixing more non-pregnancy-related ads into the circulars targeting expectant mothers. *Id.*

124. CMS maintains a national database of Medicaid claims, administered by the Medicaid Integrity Group. *See* MEDICAID INTEGRITY GRP., CTRS. FOR MEDICARE &

relatively simple approach to the problem of fraud would compare any new set of claims to the extant database of fraudulent claims. If characteristics of the new claim are too similar to characteristics of fraudulent claims, then the new claim can be flagged for further inspection.

As this example suggests, fraud detection via pattern recognition can be a powerful, but also flawed, tool. At what point is there a critical mass of similarity? Can "flagging" involve delay or hassle so severe that it ought to count as a punishment in and of itself? If so, are we comfortable as a society with meting out this punishment via a largely automated process? Finally, we must consider whether, in the interest of transparency, contractors and the public at large deserve access to the entire dataset, or whether this would merely encourage gaming the system. To elaborate on the last point, consider what might happen if writers could easily and costlessly register to run largely copied work through Turnitin, the plagiarism detection database system. They might feed this work into the system to check if their copying is detected. If so, they might alter it slightly and feed it in again, repeatedly, in order to find out what might be just enough alteration to beat the system. Policymakers would not want to allow that kind of "gaming" of a fraud detection system. On the other hand, there probably are alternative sources for much of the data, and in the absence of public access, those who are privileged or wealthy enough to access that data might essentially be able to "figure out" the system in ways that others cannot.[125]

This may seem like a merely theoretical concern, but it raises deep questions about the nature of law and the division of labor between attorneys, technologists, and auditors. To the extent we conceive of "flagging" a claim as punishment itself, the automated system is a set of rules similar to law: there is a penalty for violating it, and it is operated by entities under the aegis of state authority. On the other hand, this is a kind of detection that, like the IRS's tax audit

---

MEDICAID SERVS., COMPREHENSIVE MEDICAID INTEGRITY PLAN OF THE MEDICAID INTEGRITY PROGRAM 10 (2009), *available at* http://www.cms.gov/Regulations-and-Guidance/Legislation/DeficitReductionAct/downloads/CMIP2009-2013.pdf. Medicare claims information is centralized in the Integrated Data Repository ("IDR"), where it is available for advanced mining and analysis. *CMS Integrated Data Repository*, IT DASHBOARD, https://www.itdashboard.gov/investment?buscid=279 (last updated Aug. 30, 2013). Ultimately, CMS plans to utilize the IDR as the "single repository that [will] serve[] as the centerpiece of CMS' data needs and [will] enable cross-functional analysis" for both Medicaid and Medicare claims information. *Id.*

125. *See* Frank Pasquale, *Restoring Transparency to Automated Authority*, 9 J. TELECOMM. & HIGH TECH. L. 235, 235–36 (2011).

flags, might work optimally only to the extent that others cannot reverse engineer it.[126] We will need to think creatively about reconciling these two divergent visions of the role of automation in identifying entities and individuals for individualized attention by enforcement entities.[127]

B. Auto-Denies and Contractor Coordination

Claims reimbursement relies on proper coding and matching of submitted claims to a complex database.[128] Fraudulent entities can learn how to simulate a real practice and submit claims that look like those of an actual provider. But properly automated systems with some degree of artificial intelligence can, on the basis of past caught frauds, learn warning signs or triggers that cause "red flags" for investigators. Whereas the old model of enforcement was "pay and chase," focused on external or after-the-fact indicia of problematic behavior,[129] the hope under a regime of big data is that patterns of suspect behavior will provide a predicate for investigation.[130]

We can think of the problems for law enforcement here as one subset of a larger inquiry involving the application of artificial intelligence methods to legal scenarios. As Julius Stone noted in *The Legal System and Lawyers' Reasonings*, scholars have addressed the

126. Tal Z. Zarsky, *Transparent Predictions*, 2013 U. ILL. L. REV. 1503, 1512 (2013).

127. *See* Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 121–24 (2014) (relying on a "technological due process" model to address big data's predictive privacy harms); Neil M. Richards & Jonathan H. King, *Three Paradoxes of Big Data*, 66 STAN. L. REV. ONLINE 41, 43 (2013) (calling for a "Technological Due Process" solution to governmental and corporate decision-making by big data predictions).

128. *See* ERIC D. GERST, VULTURE CULTURE 24–25 (2008) (discussing the various problems plaguing the insurance industry). *See generally* AM. MED. ASS'N, APPEAL THAT CLAIM (2011), *available at* https://www.ama-assn.org/resources/doc/psa/appeal-that-claim.pdf (providing a step-by-step process for implementing an improved claims auditing process).

129. Lisa A. Eramo, *Stopping Fraud: Detecting and Preventing Fraud in the E-Health Era*, J. AHIMA, Mar. 2011, at 28, 28, *available at* http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_048698.hcsp?dDocName=bok1_048698 (" 'What we do now is pay and chase. You pay the bill and then do a pattern analysis to find outliers. Then you do a sting operation to recover maybe a million or billion dollars. . . . This is a drop in the bucket. We're talking about a $250 billion problem.' " (quoting Donald W. Simborg, M.D., independent health IT consultant)).

130. *See* VICTOR MAYER-SCHONBERGER & KENNETH CUKIER, BIG DATA 27–28 (2013); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, 76 TEX. L. REV. 553, 572 (1998) ("Technological standards [on the Internet] may be designed to prevent actions from taking place without the proper permissions or authority.").

automation of legal processes since at least the 1960s.[131] It is difficult to successfully balance the imperatives of efficiency and basic legal values of regularity, fair play, and due process. Automation of contracts and even dispute resolution promises to add a great deal to productivity.[132] On the other hand, we already have seen disastrous failures of automation, ranging from failures of record keeping during the housing crisis[133] to the frightening "flash crash" in stock trading in 2010.[134]

Coordination problems between CMS and the various contractors fall somewhere in between these two conflicting results. New vistas of fraud detection have arisen, but notable failures are also clear. For example, the community mental health sector has come under well-justified scrutiny, but contractors have not cracked down with sufficient alacrity and celerity.[135] For example, in one case a contractor determined that providers were billing for extensive partial hospitalization services.[136]

How precise can these entities become? It is helpful to de-familiarize the fraud context and think about the computability of legal determinations in general. The very idea of "computing" a legal obligation may seem strange at the outset, but law professor Harry Surden's work on computability acclimates us to it by carefully explaining several concrete, real-world examples.[137] Drawing from the world of finance, derivative contracts, and copyright licenses, he shows how humans can structure data in order to make it meaningful

131. *See* JULIUS STONE, LEGAL SYSTEM AND LAWYERS' REASONINGS 37–41 (1964) ("[E]xperiments are proceeding in the use of electronic computers as aids to legal memory, analysis and thought.").

132. *See* Harry Surden, *Computable Contracts*, 46 U.C. DAVIS L. REV. 629, 689–90 (2012).

133. *See* Danielle Douglas, *New Rules Are Set to Curb Abuses by Mortgage Servicers*, WASH. POST, Jan. 17, 2013, at A15.

134. *See* U.S. COMMODITY FUTURES TRADING COMM'N & U.S. SEC. & EXCH. COMM'N, FINDINGS REGARDING THE MARKET EVENTS OF MAY 6, 2010, at 13–14 (2010) (discussing factors that led to the "flash crash").

135. For example, in Florida, some providers were serviced by a MAC/ZPIC and others were serviced by a FI/PSC. *See* DEP'T OF HEALTH & HUMAN SERVS., *supra* note 86, at 20.

136. *Id.* at 21. Partial Hospitalization Program ("PHP") services are "intense, structured outpatient mental health treatment programs," which are "particularly vulnerable to fraud, waste and abuse." *Id.* at 1–2. The MAC/ZPIC team serving the region identified the suspected providers and beneficiaries. *Id.* at 14. The MAC initiated an "auto-deny" to prevent future payments, but the fiscal intermediary for the region did not. *Id.* at 20–21. Thus the providers took another $520,000 after the MAC had tried to stop payments. *Id.* at 20.

137. *See* Surden, *supra* note 132, at 659–63.

for computer software.[138] For example, a DVD may be licensed for play only in the United States and Europe and then be "coded" so it can play only in those regions and not others.[139] Were a human playing the DVD for the user, he might demand a copy of the DVD's terms of use and receipt to see if it was authorized for playing in a given area. Computers need such a term translated into a language they can "understand"; or, to put it another way, the legal terms embedded in the DVD must lead to predictable reactions from the hardware that encounters them.[140]

Surden explains the promise (and importance) of computable contracts in a world where machines are increasingly monitoring (and even creating) the real "states of the world" that trigger various contractual terms.[141] Practitioners are creating shared meaning in computational systems by building up, step by step, a community's understanding of the types of "givens" needed for such systems to work—including "captured legal assertions" that encode a human professional's assessment of a given situation, such as: no podiatric claims for "clipped nails" should include over twenty clipped nails per patient per day. This is what is necessary for legal computation to function in positive and predictable ways.

Such foundational concerns are relevant to ongoing challenges in the medical field's adaptation of HIT. For example, one EHR system may be able to understand "C," "cgh," or "koff" as "cough," and may well code it in any way it chooses. But to integrate and to port data, all systems need to be able to translate a symptom into a commonly recognized code. Health care providers can avoid getting "locked into" a system only if they can transport their records from one vendor to another. Patients want their providers to seamlessly integrate records. Assuring there is one universally useful record that can be processed by diverse parties is a critical aspect of health record adoption and improvement. This process of standardization and translation is also critical to an increasing number of legal scenarios. Well-defined syntax and semantics are an increasing concern for health and finance regulators.

---

138. *Id.*

139. *See* Peter K. Yu, *Region Codes and the Territorial Mess*, 30 CARDOZO ARTS & ENT. L.J. 187, 194–95 (2012) (explaining the technology behind DVD region codes).

140. *See* Harry Surden, *The Variable Determinacy Thesis*, 12 COLUM. SCI. & TECH. L. REV. 1, 7–8 (2011) (noting that creating "accurate computer models of the substantive rules and factors implicated in legal decision-making" has been successful in certain contexts where legal rules are well established ex ante, such as tax law).

141. *Id.* at 4.

Unfortunately, digitization can also be a "force multiplier" when it comes to fraud.[142] New technology can supercharge fraudulent billing practices.[143] EHR systems include certain timesaving software tools, such as copy and paste functions, that increase the efficiency of health care delivery. However, these tools also can be used to commit fraud faster and with greater ease than ever before.[144] This vexing issue may undermine the cost savings that have been promised regarding electronic health records.[145]

C. *Variation in Medicare Administrative Contractor Effectiveness*

The use of EHRs "makes it faster and easier [for providers] to be fraudulent,"[146] but has not yet uniformly empowered fraud contractors to detect such fraud. Home health care agencies are another fraud-prone medical service where Medicare contractors have shown inconsistent efforts and correspondingly variable successes.[147] Regional variations are pronounced.[148] The MAC for Area A, which services significantly less home health agencies than the MAC for Area C,[149] accounted for almost all of the prevented payments.[150] ZPICs were also inconsistent in their investigation and

142. *See* FOUND. OF RESEARCH & EDUC., AM. HEALTH INFO. MGMT. ASS'N, REPORT ON THE USE OF HEALTH INFORMATION TECHNOLOGY TO ENHANCE AND EXPAND HEALTH CARE ANTI-FRAUD ACTIVITIES 13 (2005) ("Without a deliberate effort to build fraud management into [electronic systems], healthcare payers and consumers will be exposed to new and potentially increased vulnerability to electronically-enabled healthcare fraud.").

143. *See* Donald W. Simborg, *There Is No Neutral Position on Fraud!*, 18 J. AM. MED. INFORMATICS ASS'N 675, 676 (2011).

144. *See generally* Eramo, *supra* note 129, at 28–29 (discussing the need for better systems to detect and prevent false claims).

145. *See* Fred Schulte, *Growth of Electronic Medical Records Eases Path to Inflated Bills*, CENTER FOR PUB. INTEGRITY (Sept. 19, 2012, 6:00 AM), http://www.publicintegrity.org/2012/09/19/10812/growth-electronic-medical-records-eases-path-inflated-bill; Simborg, *supra* note 143, at 675.

146. *See* Reed Albeson, Julie Creswell & Griffin J. Palmer, *Medicare Bills Rise as Records Turn Electronic*, N.Y. TIMES, Sept. 22 2012, at A1 (internal quotation marks omitted).

147. *See* OFFICE OF INSPECTOR GEN., *supra* note 113, at 2, 13–18 (reporting a study of contractor results in preventing fraud in home health care).

148. *Id.* at 13.

149. MAC A's region included 326 home health agencies in 2011, while MAC C's region had 6,812. *Id.* at 14.

150. *Id.* at 13. Both MACs appear to be using external and internal fraud investigation techniques, so it is unclear why MAC A had more success. It is possible that the difference in the number of home health agencies combined with the number of fraud-prone geographical areas overwhelmed MAC C, but MAC C did not cite this as a concern.

prevention of home health agency fraud.[151] But pushback also comes from the other direction: from those who are concerned that ZPICs are demanding too much in their quest to reduce fraud. Their investigations have been called "the Wild West, because . . . there's no real due process, there are no real checks and balances."[152] There appears to be no limit to the number of requests for additional documentation each ZPIC can require from providers, no notice of outcome requirement, and no opportunity to discuss a denial with a medical director.[153] In an informal conversation with a practitioner in North Carolina, I learned that some of her clients are waiting over twenty-five months for "telephonic hearings" with administrative law judges.[154] Both MACs and ZPICs can deny claims for what may be very subjective judgments, such as "illegible physician signatures or dates."[155] There also are inconsistent methods and approaches used by diverse contractors. Instead of trying to develop methods for unifying and simplifying the review process, CMS has opted to develop trainings for providers.[156]

Admittedly, CMS faces a difficult task here. It is caught between advocates who will charge it with doing too little, and those who believe it is doing too much. The old standards for investigations need to be updated for the digital age. For example, consider the post-payment reviews done by RAs.[157] At first, CMS gave the RAs very strong incentives to find problematic practices, ordering that they could keep between nine and twelve and one-half percent of the funds they recovered, regardless of whether the claim was upheld on appeal.[158] Unfortunately, many of the resulting investigations

151. *Id.* at 15. As with the investigations of community mental health centers discussed previously, the Zone 7 ZPIC had by far the most investigations of home health agencies, more than double the combined number of investigations of the other ZPICs in the study. *Id.* at 16. Zone 4 had the second highest number of investigations, but also covers almost double the number of providers as does Zone 7. *Id.* at 17. The delay resulted in continued payments, totaling over $650 million. *Id.* Based on these findings, CMS responded that it would modify the contractors' statements of work to "clarify [the] processes" ZPICs use to screen high-risk providers. *Id.* at 21.

152. *House Panel Considers CMS' Medicare Fraud-Prevention Efforts*, GOV'T CONTRACTOR, JUNE 27, 2012, at 1, 1 (internal quotation marks omitted).

153. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 90, at 22.

154. Interview with North Carolina practitioner (Oct. 4, 2013). Due to the potential sensitivity of client relations, I am respecting the practitioner's anonymity.

155. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 90, at 21–22. RAs can deny claims only based on reasonableness or lack of medical necessity. *Id.* at 22–24.

156. *Id.* at 32.

157. *See generally id.* at 19 (discussing post-payment reviews done by RAs).

158. *Id.*

ultimately failed to reveal any wrongdoing on appeal.[159] CMS then changed course, ordering that RAs are not to be compensated if the determination of overpayment is reversed on appeal, as well as setting other limits on them.[160]

Despite that concession, the American Hospital Association ("AHA") is still not satisfied. It claims the audit process violates the Medicare Act.[161] As a result of the audits, the AHA maintains, hospitals have lost hundreds of millions of dollars and face financial "uncertainty" that "ultimately may adversely affect patient care."[162]

The audit process can be very burdensome for some institutions.[163] A recent case involving Gentiva Healthcare Corporation, which operated a home health care agency called Heritage Home Health, is instructive.[164] Initially charged with overbilling by $4,242,452.10, Gentiva was actually responsible for just $850,000 in overpayments.[165] That determination took six years from the date of the initial review[166] and unknown expenditures of

159. *Id.*

160. *See* Memorandum from the Inspector Gen. to the Sec'y of DHHS, *supra* note 110.

161. Complaint at 1–2, Am. Hosp. Ass'n v. Sebelius, No. 12-cv-01770-CKK (D.D.C. filed Nov. 1, 2012), 2013 WL 2474428. The AHA charges that RAs are deeming medically necessary care improper if the care was provided in a hospital but could have been provided in an outpatient setting. *Id.* at 2–3. The AHA has argued that "when a hospital furnishes reasonable and medically necessary items and services, if payment cannot be made under Part A, it must be made under Part B," but the latter payment may be delayed or not happen at all due to the complexity of the audit process. *Id.* at 4.

162. *Id.* The Secretary has moved for the case to be dismissed because, among other reasons, the plaintiffs are still pursuing administrative remedies and the Secretary has not issued a final rule. *See* Defendant's Memorandum of Points and Authorities in Support of Her Motion to Dismiss for Lack of Subject Matter Jurisdiction and Failure to State a Claim upon Which Relief Can Be Granted at 3, Am. Hosp. Ass'n, v. Sebelius, No. 12-cv-01770-CKK (D.D.C. June 6, 2013), 2013 WL 2474428. The Secretary, however, later amended the rule so that hospitals that had pending appeals could be compensated, but not those whose appeals had run, a remedy the AHA finds to be an "administrative shell game" that does not address the concerns of hospitals that have lost payments in the past. Plaintiffs' Opposition to Defendant's Motion to Dismiss at 1–2, Am. Hosp. Ass'n, v. Sebelius, No. 1:12-cv-1770-CKK (D.D.C. June 27, 2013), 2013 WL 2474428 (citation omitted).

163. *See* Grigg, *supra* note 83.

164. *See* Gentiva Healthcare Corp. v. Sebelius, 857 F. Supp. 2d 1, 2–3 (D.D.C. 2012), *aff'd*, 723 F.3d 292 (D.C. Cir. 2013).

165. *Id.* at 4–5. The main issue in *Gentiva* was the contractor's determination of a "sustained or high level of payment error," which Gentiva argued could not be delegated to a contractor based on the statute. *Id.* at 2. The court disagreed and found that the delegation was within the Secretary's authority and that Congress had expressly preempted judicial review of the determination. *Id.*

166. *See id.* at 2 (stating that the initial review took place in 2007).

resources.[167] When the Department of Justice ("DOJ") and DHHS trumpet figures about how much new fraud deterrence measures have saved taxpayers, they must do a better job of accounting for the costs these measures visit on providers.[168] Hard-pressed and stressed thanks to various cost-cutting pressures in the ACA, as well as larger economic trends, providers do not deserve to be burdened by protracted, expensive legal conflicts over genuine claims.

CONCLUSION

CMS uses private contractors extensively. In terms of its investigation and prevention of fraudulent billing activities, its contractors have shown inconsistent efficacy in performing their delegated duties. The post-payment auditing process in particular has become the subject of legal action as providers attempt to avoid substantial payment recoupments. In addition to the burden of legal action, the lack of CMS oversight has allowed private contractors to create conflicting and difficult requirements for providers. Because of these questionable activities and the uneven benefits, the use of private contractors for Medicare fraud prevention and investigation should be thoroughly scrutinized to assure that the time and money invested in enforcement is worth the amount recouped, discounted by the amount of unnecessary time, worry, and expense imposed on providers via the enforcement and audit process.

For "front end" investigation of HIT, the ONC has enjoyed more success with ATCBs. The delegation process of authority to ATCBs is complex, and admittedly, these entities have begun as modes of qualifying providers for subsidies. However, lack of meaningful-use-certified software will eventually lead to financial penalties, and we should not overstate the difference between subsidy and penalty in the marketplace even now—money is fungible and can be leveraged to provide critical advantages over competitors.

---

167. *Cf.* Christopher Young, *Technical Component Laboratory Pathology Services: Who Bills? Know the Rules and Regulations and Make Sure You Have Systems in Place to Respond Quickly*, 12 J. HEALTH CARE COMPLIANCE 61 (2010) (describing a specific incident in which the RAC ultimately withdrew the audit but only after "both providers and the A/B Medicare administrative contractor (MAC) have had to expend resources responding to the audit and then repairing the damage").

168. For example, the DOJ promoted a case in which HCA Inc. settled for $1.7 billion after being accused of improper billing and referral. *See* Press Release, U.S. Dep't of Justice, Largest Health Care Fraud Case in U.S. History Settled, HCA Investigation Nets Record Total of $1.7 Billion (June 26, 2003), *available at* http://www.usdoj.gov/opa/pr/2003/June/03_civ_386.htm. The DOJ should have balanced this settlement recovery with the dollars lost to providers in their efforts to prepare for non-meritorious fraud claims.

The central theme of complaints against anti-fraud contractors is the post hoc nature of investigations. For providers, long waits for due process can disrupt revenue cycle management and sometimes even threaten the viability of their own enterprise. For fraud watchdogs, there are too many missed opportunities to stop egregious behavior.[169]

I predict that, in the coming decade, there will be growing pressure to integrate features of fraud detection, public health surveillance, and comparative effectiveness research into HIT at the certification stage. Admittedly, such multidimensional programming may generate some slow and buggy "bloatware" ill-suited for high-pressure, high-paced hospital environments. But if the pressures of responding to ZPICs, RACs, and other audit contractors become too high, providers themselves may try to preempt investigation by building in fraud-fighting tools at the front end.

Many experts in the HIT field have been disappointed by information technology's failure to "disrupt" health care—that is, to establish efficiencies and new modes of diagnosis and treatment that are radically cheaper (and make care far more accessible) than the presently dominant modes of care.[170] For some, the hope is that massive information companies like Apple or Google will come in, *a la deus ex machina*, to transform the medical industry the way they have already impacted music and search.

Unfortunately for this line of reasoning, Google has already tried (and failed) in this space with Google Health.[171] Apple sells many health apps, but does not appear to be getting into the business of integrating data from them into extant electronic medical records or even personalized health records. Neither company appears interested in routine improvement of health outcomes, however much "singularitarianism" may appeal to Silicon Valley CEOs.[172]

---

169. *See House Panel Considers CMS' Medicare Fraud-Prevention Efforts*, *supra* note 152; Schulte, *supra* note 145; Simborg, *supra* note 143, at 676.

170. *See* Terry, *supra* note 23, at 742. Harvard Business School professor Clayton Christensen, for instance, suggests that the "Innovator's Prescription" largely relies on private firms. *See* CLAYTON M. CHRISTENSEN, THE INNOVATOR'S PRESCRIPTION: A DISRUPTIVE SOLUTION FOR HEALTH CARE 195–98 (2009).

171. *See* David Talbot, *How a Broken Medical System Killed Google Health*, MIT TECH. REV., June 29, 2011, *available at* http://technologyreview.com/news/424535/how-a-broken-medical-system-killed-google-health/ (noting that Google "is unwilling, for perfectly good business reasons, to engage in block-by-block market solutions to health-care institutions one by one . . . and expecting patients to actually do data entry is not a scalable and workable solution" (internal quotation marks omitted)).

172. *See* Frank Pasquale, *Two Concepts of Immortality*, 14 YALE J.L. & HUM. 73, 84 (2002) (exploring "regenerative and genetically engineered models of health") (internal

Other historians and economists of innovation would instruct us to look to the government, rather than private industry, to take the lead here. Vernon Ruttan's work has focused on the Defense Department's critical role in funding innovations like interchangeable parts and Internet connectivity.[173] The more one knows about the intertwining of state and market in health care, defense, telecommunications, energy, and banking, the less realistic any strict divide between "public" and "private" appears. Moreover, even the Internet sector, that last bastion of venture capital and risk taking, is more a creature of state intervention than market forces.[174]

Whoever is "in the driver's seat," we can be assured that public-private partnerships are a permanent feature of our health system's landscape. The questions now are how to move beyond the problems emerging in key areas (like IT certification and fraud detection) and how to better calibrate responses to suboptimal medical practice. As cost pressures continue, the seamless integration of clinical decision support, revenue cycle management, and fraud detection will become a "holy grail" for both policymakers and actors in the private sector.

---

quotation marks omitted)); Jane Wakefield, *Singularity University Plots High Tech Future for Humans*, BBC NEWS (Dec. 2, 2013, 7:17 PM), http://www.bbc.co.uk/news/technology-25000753 (discussing immortalization as Silicon Valley's *ideé fixe*).

173. *See* VERNON W. RUTTAN, IS WAR NECESSARY FOR ECONOMIC GROWTH? 5–8 (2006).

174. *See* Mariana Mazzucato, *It's a Myth that Entrepreneurs Drive New Technology*, NEWSCIENTIST (Sept. 1, 2013, 5:00 AM), http://www.slate.com/articles/health_and_science/new_scientist/2013/09/entrepreneurs_or_the_state_innovation_comes_from_public_investment.html. Professor Mazzucato notes as follows:

> Whether an innovation will be a success is uncertain, and it can take longer than traditional banks or venture capitalists are willing to wait. In countries such as the United States, China, Singapore, and Denmark, the state has provided the kind of patient and long-term finance new technologies need to get off the ground.... Apple is a perfect example. In its early stages, the company received government cash support via a $500,000 small-business investment company grant. And every technology that makes the iPhone a smartphone owes its vision and funding to the state: the Internet, GPS, touch-screen displays, and even the voice-activated smartphone assistant Siri all received state cash. The U.S. Defense Advanced Research Projects Agency bankrolled the Internet, and the CIA and the military funded GPS. So, although the United States is sold to us as the model example of progress through private enterprise, innovation there has benefited from a very interventionist state.

Id.